SP.GOV.BR

SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS

# CIBERSEGURANÇA

## Guia de boas práticas

# INTRODUÇÃO

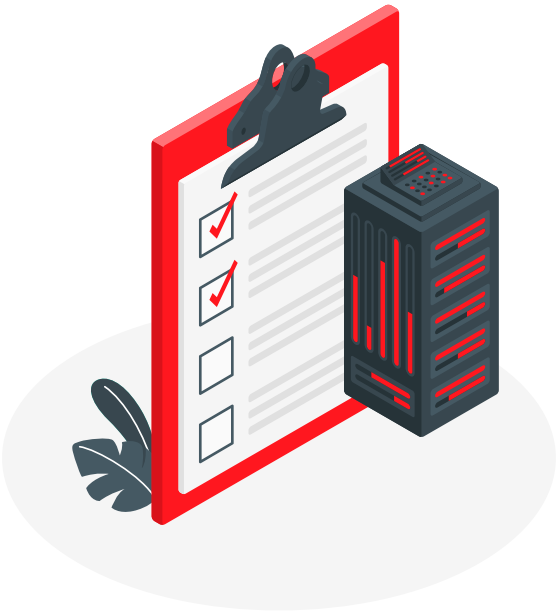
A Secretaria de Gestão e Governo Digital do Estado de São Paulo, criou o Guia de Boas Práticas em Cibersegurança para melhorar a segurança digital na Administração Pública Estadual.

Este Guia oferece orientações para que os órgãos e entidades adotem práticas que protejam plataformas, sistemas e estruturas importantes, garantindo que os serviços públicos continuem funcionando. Ele está alinhado com as melhores práticas do Brasil e do mundo, promovendo a conscientização sobre a importância da cibersegurança e facilitando a implementação de ações para prevenir e responder a ameaças. O Guia também recomenda que sejam feitos diagnósticos periódicos e avaliações regulares do nível de segurança, seguindo diretrizes claras para gerenciar riscos, com base em princípios como defesa em profundidade e colaboração entre órgãos.

A atualização do Guia acontece regularmente para se manter em sintonia com as inovações tecnológicas, fortalecendo a segurança cibernética do Estado de São Paulo.

São Paulo são todos!

# SUMÁRIO



# 01. BASE LEGAL


## Estratégia de Governo Digital (EGD), aprovada pelo Decreto n° 67.799, de 13 de julho de 2023, que prevê:

**1.** Investimento contínuo em soluções tecnológicas para proteger dados e informações.
*(Artigo 3º, inciso VI)*

**2.** Uso da tecnologia para identificar, prevenir e punir práticas de corrupção, fraude e outros crimes.
*(Artigo 3º, inciso VII)*

**3.** Aprimoramento constante de infraestrutura e segurança dos recursos de tecnologia da informação e comunicação
*(Artigo 4º, inciso XIII)*

**4.** Medidas de segurança digital inclusas nos Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs)
*(Artigo 5º, inciso I, alínea "d")*

**Papel da SGGD**
Coordenar a implementação da EGD
*(Artigo 6º, inciso II)*

**Papel da PRODESP**
Fornecer serviços de tecnologia da informação e comunicação para a execução da EGD e dos PDTICs
*(Artigo 7º)*

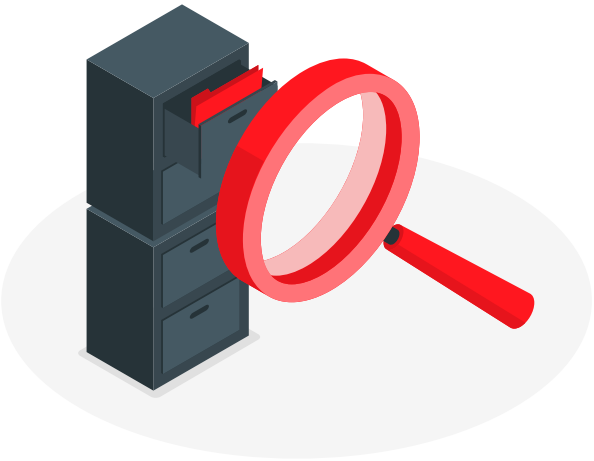
# 02.
# DISPOSIÇÕES PRELIMINARES

## Este Guia pretende:

**Orientar Órgãos Públicos**
Os órgãos e entidades da Administração Pública Estadual serão orientados a adotar práticas que melhorem a segurança cibernética.

**Facilitar Medidas de Segurança**
É importante facilitar a implementação de ações para prevenir e responder a ameaças cibernéticas, com o objetivo de proteger sistemas e infraestruturas críticas do Estado.

# 03. TERMOS IMPORTANTES



## Para compreender este Guia, considere as seguintes definições:

**Cibersegurança**

Conjunto de práticas e medidas que protegem sistemas, redes e dados, garantindo que as informações sejam mantidas confidenciais, íntegras e disponíveis quando necessário.

**Diagnóstico de Cibersegurança**

Avaliação que verifica como está a segurança de um órgão ou entidade, identificando pontos fracos (vulnerabilidades), possíveis ameaças e riscos em seus ativos tecnológicos.

**Avaliação de Maturidade em Cibersegurança**

Análise que mede a capacidade do órgão em implementar, gerenciar e melhorar controles de segurança, usando modelos reconhecidos como o NIST Cybersecurity Framework e das 7 Camadas de Segurança.

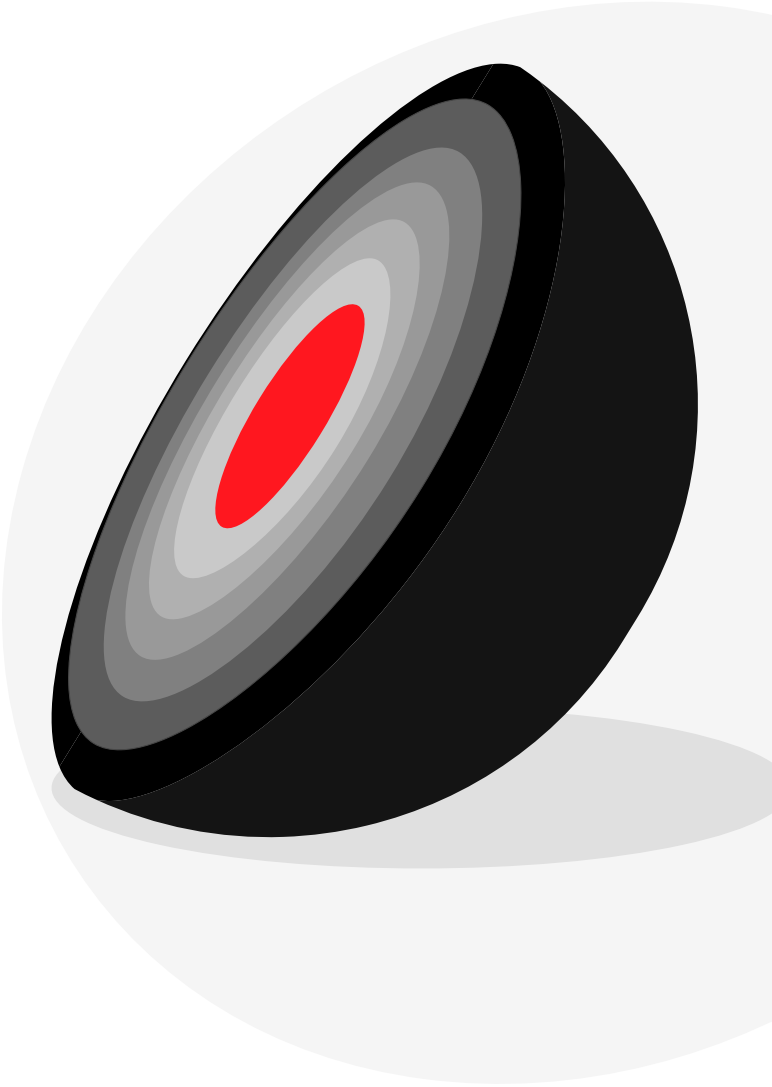
**NIST Cybersecurity Framework**

Conjunto de diretrizes e boas práticas criado pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), que oferece uma abordagem estruturada para gerenciar riscos cibernéticos, ajudando as organizações a identificar, proteger, detectar e responder a incidentes de segurança.

**Modelo das 7 Camadas de Segurança**

Recomenda a implementação de várias camadas de proteção, seguindo o princípio de **Defesa em Profundidade**, para garantir a segurança de sistemas, redes e dados. As camadas são:

- **Camada de Perímetro**: Protege a fronteira entre a rede interna e o mundo externo, impedindo acessos não autorizados.
- **Camada de Rede**: Protege o tráfego de dados dentro da rede, controlando a comunicação interna e identificando ameaças.
- **Camada de Aplicação**: Protege os programas e aplicações contra falhas e acessos indevidos, garantindo que funcionem de forma segura.
- **Camada de Endpoint**: Protege os dispositivos que acessam a rede (como computadores e celulares) contra malware e acessos não autorizados.
- **Camada de Ativos Críticos**: Protege sistemas e servidores essenciais para a operação, assegurando que estejam protegidos contra ataques e falhas.
- **Camada Humana:** Foca na conscientização e treinamento dos usuários para evitar erros humanos e comportamentos de risco.
- **Camada de Dados**: Protege os dados armazenados e em trânsito, garantindo que estejam seguros contra acessos não autorizados e vazamentos.



**Vulnerabilidade**

Uma fraqueza que pode ser explorada para comprometer a segurança de um sistema.

**Ameaça Cibernética**

Evento ou ação que pode causar danos a sistemas ou informações.

**Risco Cibernético**

A chance de uma ameaça explorar uma vulnerabilidade, causando um efeito negativo.

**Ativo**

Qualquer recurso valioso para a organização, incluindo informações, sistemas e pessoas.

**Impacto**

Consequência negativa resultante da exploração de uma vulnerabilidade, como perdas financeiras, interrupção de serviços, danos à reputação ou vazamento de dados.

# 04.
# PRINCÍPIOS

## As boas práticas em cibersegurança devem estar alinhadas aos seguintes princípios:

**Abordagem Sistêmica**
Considerar todos os aspectos da segurança da informação de forma integrada e conjunta.

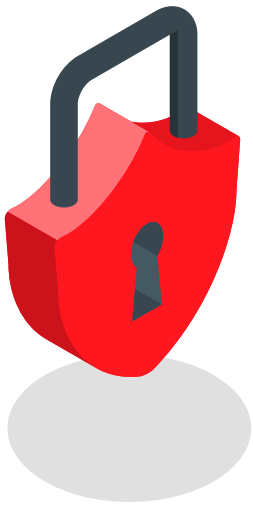
**Gestão de Riscos**
Identificar e reduzir continuamente os riscos cibernéticos.

**Defesa em Profundidade**
Implementar várias camadas de segurança para uma proteção mais forte.

**Cooperação**
Colaborar com outros órgãos e entidades para compartilhar informações e estratégias de segurança.

**Cultura de Segurança**
Promover valores e comportamentos que colocam a segurança como prioridade em todas as atividades.

# 05. DIAGNÓSTICO



**Buscando elevar a maturidade e a resiliência em segurança cibernética, a Resolução 33/2024 recomenda que os órgãos e entidades realizem diagnósticos periódicos de cibersegurança, observando alguns passos fundamentais:**

**Análise de Vulnerabilidades**
Identificar fragilidades em sistemas, aplicações e rede.

**Avaliação de Risco**
Analisar o impacto e a probabilidade das vulnerabilidades.

**Análise de Superfície de Ataque**
Mapear possíveis pontos de entrada para ataques.

**Monitoramento de Tráfego**
Observar a rede para detectar atividades suspeitas.

**Análise de Logs**
Examinar registros para identificar eventos suspeitos.

## Como o diagnóstico funciona

*Com o apoio da PRODESP, os órgãos públicos poderão avaliar sua maturidade em cibersegurança por meio da Análise de Risco Cibernético (ARC), uma ferramenta que utiliza as sete camadas de segurança digital, baseadas no Modelo de Interconexão de Sistemas Abertos (OSI). A avaliação abrange uma análise detalhada das práticas de segurança adotadas, a verificação das superfícies de ataque e a identificação do percentual de risco cibernético presente.*

**Camada de Perímetro**

A PRODESP verificará a proteção na borda da rede, incluindo a utilização de firewalls e outras ferramentas que defendem os ativos expostos, como portais de acesso e serviços de internert.

* ***A avaliação analisará a existência e a configuração de firewalls e mecanismos de proteção contra vulnerabilidades em ativos expostos ao público.***

**Camada de Rede**

Serão analisados os controles de visibilidade sobre os ataques que ocorrem na rede interna, verificando se há ferramentas e procedimentos para monitorar e identificar atividades suspeitas ou tentativas de intrusão.

* ***A verificação incluirá o nível de controle sobre ataques e tráfego dentro da rede.***

**Camada de Aplicação**

A avaliação se concentrará na segurança de acessos privilegiados e na proteção das credenciais armazenadas em aplicações corporativas, como senhas em navegadores e dispositivos móveis.

* ***Será avaliada a proteção de acessos privilegiados e de credenciais armazenadas em aplicações.***

**Camada de Humana**

Serão verificadas a maturidade dos usuários em relação à segurança cibernética, o uso de autenticação multifator em aplicações web e a existência de auditoria de acessos e análise de comportamento.

* ***A avaliação buscará aferir o nível de conscientização e a capacidade de detectar e prevenir comportamentos de risco.***

**Camada de Endpoint**

A proteção dos dispositivos finais, como computadores e celulares, será avaliada, verificando se há soluções

adequadas para prevenir ataques e se as credenciais dos usuários estão protegidas contra roubo ou uso indevido.

* ***A análise focará na segurança dos endpoints e na proteção das credenciais dos usuários nesses dispositivos.***

**Camada de Missão Crítica**

A segurança dos servidores críticos será avaliada, examinando as soluções de proteção contra ataques cibernéticos e a segurança das credenciais utilizadas nos servidores.

* ***A análise focará na segurança dos endpoints e na proteção das credenciais dos usuários nesses dispositivos.***

**Camada de Dados**

Será avaliado o controle de acesso aos dados armazenados, bem como as políticas de segurança que garantem a confidencialidade, integridade e disponibilidade das informações.

* ***A verificação incluirá a segurança dos dados e os controles de acesso às informações armazenadas.***

## Próximos Passos

*Após concluir o diagnóstico e a avaliação de maturidade em cibersegurança, a Prodesp poderá elaborar um relatório que inclua:*

**Resultados Encontrados (Prodesp)**
Detalhe de todas as vulnerabilidades e riscos identificados. Isso ajudará a entender exatamente onde estão os pontos fracos que precisam ser corrigidos.

**Recomendações de Cibersegurança (Prodesp)**
Identifique medidas para mitigar os riscos e corrigir as vulnerabilidades. Isso pode incluir atualizações de software, melhorias nos processos ou treinamentos para a equipe.

**Plano de Ação (Órgão)**
Proponha um cronograma com etapas claras e defina quem será responsável por cada ação. Isso garantirá que as melhorias sejam implementadas de forma organizada e eficiente.

# 06. RECOMENDAÇÕES

## Recomenda-se que os órgãos sigam as orientações abaixo:

**Implementar Medidas do Diagnóstico**
Aplicar as medidas identificadas no plano de ação elaborado;

**Investir em Capacitação**
Promover treinamento e conscientização dos colaboradores sobre segurança digital e práticas seguras.

**Desenvolver Planos de Resposta a Incidentes**
Estabelecer procedimentos claros para agir de forma eficiente em caso de incidentes cibernéticos.

**Atualizar Sistemas Regularmente**
Garantir que todos os softwares e dispositivos estejam com as últimas atualizações e correções de segurança.

**Controlar Acessos e Identidades**
Gerenciar rigorosamente o acesso a sistemas e informações, implementando senhas fortes e autenticação multifator.

**Monitorar Ativamente**
Implementar soluções de monitoramento contínuo para detectar e responder rapidamente a ameaças e incidentes.

Em caso de dúvidas, envie um e-mail para o endereço eletrônico ciberseguranca@sp.gov.br.


SP.GOV.BR
SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS